BIOMETRIC CONSORTIUM
KEYNOTE SPEECH BY DR. JOSEPH J. ATICK
FEBRUARY 13, 2002 – WASHINGTON, DC

Good morning everyone and thank you for coming. Before I begin this talk, I would like to thank NIST; I would like to thank the NSA and the organizing committee of this conference. Specifically, I would like to thank Jeff Dunn, for giving me the honor to deliver the keynote speech at what I believe has emerged as a milestone event in the history of the Biometric Consortium. I have been attending these Biometric Consortium conferences for eight years now and this is the most impressive crowd I have seen.

The topic of today's speech is that which has occupied our nation for the last five months. Namely, homeland security, and how biometrics fits into our homeland security objectives. This is an issue that I predict will consume us for quite some time.

My objective today is to give you an overview of the role biometrics play in homeland security and to lay the foundation for the detailed analyses and discussions for the other speakers throughout this conference.

Paradigm Shift

I start by telling you about the things you already know. The tragic events of September 11 have forced a major realignment in our nation's security and defense priorities. Many expect the impact on domestic and foreign policy to be indefinite. And many expect that biometrics will be a central component to our homeland defense strategy for years to come. From an industry perspective, we are justified in asking, are witnessing a paradigm shift? I think the subject is worth exploring in a couple of slides.

Let us examine the conditions that had prevailed prior to September 11. Prior to September 11, we were an industry in search of a compelling mass application. Our value proposition was not clearly appreciated. We talked about security; the world did not listen. Convenience was the prevailing factor we tried to promote forward, but convenience was a value proposition that could only go so far.

We also had multiple adoption barriers – to name a few: privacy concerns, lack of political will, lack of funding, lack of infrastructure. After September 11, ID technologies such as biometrics have become critical in our defense against terrorism. Safety and security have become clear and prevalent value propositions. We have seen federal legislation be adopted. We have seen accelerated funding, security mandates and a significant shift in public opinion that is favoring biometrics.

In my opinion, however, the most remarkable change is in the political will. We have an Administration that is committed; that has embraced the cause for the security of the American public and this is an Administration that is looking to adopt technology, because it cannot afford to fail in this highly visible task. So I think it is safe to say that the political will is strongly in favor of security and ID systems.

What we are here to talk about, and what I will present therefore, is a vision of what the industry believes is the vital role that biometrics can play in our national security efforts.

My challenge is that my audience consists of two types of people. For those who represent government agencies, I would like to set forth several recommendations that you may take with you. To the industry, I would like to highlight some of the opportunities and more importantly, some of the challenges that we have to meet. If I succeed, the credit goes to the industry for being proactive in articulating how biometrics can work in this regard. If I fail, the blame is entirely mine and I hope the speakers today and tomorrow will rectify the shortfall.

So here I present you with a framework – with what I, perceive the framework for homeland security to be.

The Biometric Platform for Homeland Security

I think the time has come for us to move away from thinking about security in terms of fencing doors and borders and to start thinking about enabling and preventing actions in a more human-centric framework. Essentially, this is the notion of associating identity with action and credentials. This has to be the core of our mission.

Why? Because, in our mission, we are trying to prevent the actions of those who threaten public safety, while facilitating the actions of the honest majority. If you think about this one phrase, all actions are linked to an individual's identity. Let me share some examples with you. The way we prevent the actions of those who threaten public safety is to conduct a risk assessment on what actions have potential for massive effects. I am not advocating for government management in every action we conduct. I am talking about actions that matter. Who lives in this country? Who leaves this country? Which guests and visitors are granted access into this country is something that matters. We need to conduct an analysis to set what are the actions that have mass effects. But for the purposes of this discussion, I will assume we have done that.

We also need to consider the notion of what I call the "trusted identity". The "trusted identity" is what I have often referred to as the honest majority and is a term that I would like to explore further. I will come back to this later in my presentation.

First, it is important to take a step back and realize that in order to accomplish the security objective of associating action with credentials and identity, it is necessary to develop several inter-operable information sub-systems. Further, I claim that these sub-systems all have to work together as part of a platform, with multiple components that can operate on their own but at the same time be able to connect with the other sub-systems in order to deliver an overall solution.

I see four sub-system components of this platform – knowledge and data; background checking systems; privileged access; watch-list detection.

Before I go into discussion of what I think these sub-systems should do, I would like to say a couple of words about the role of biometrics. First, if you examine each and every one of those systems, you find underlying them is a biometrics capability. For example, to do a background check implies performing a one-to-many search with biometrics. To gain privileged access, implies a one to one verification of the "trusted identity". When setting up the databases, you need to do a one-to-many search for combating fraud. To detect criminals and terrorists, you need to do a one to few search in real time to match against watch lists. So each and every one of the sub-systems I had previously outlined are actually parts of a platform enabled for biometrics.

I would like to make another point. When we think about the task that we are faced with as a nation, I hope we are not going to get caught up in the details of developing the specific sub-systems now. I think in all probability, we are going to get them wrong in the first implementation. What we need to do first and foremost as the national priority is to develop the platform in which the sub-systems will operate. And equally important, we need to develop standards that will allow complex systems to be built from well-defined inter-operable system modules. Again, I have already named the system modules that exist. They exist in systems that the federal government has been implementing but they need to be tied to one another as part of a platform.

Sub-System Components

Let us begin by talking about the knowledge and data sub-system. As you all know, crime and terror have identities. There is a wealth of data that can be tapped on, whether from local, federal or international sources. The logos on this slide represent 15 international agencies that for the last 30 years or so have been collecting data on terrorists, criminals, fugitives, drug traffickers, etc. If you can name all 15 by recognizing their logos, your eyes must be as powerful as James Bonds' or you work for one of these agencies. In any case, the fact that these agencies exist, challenges us to improve data gathering and intelligence.

President Bush made this case in his State of the Union address last month. We need to improve data gathering mechanisms. But more importantly, we need to facilitate the sharing of the data that we do have. There is a wealth of information that exists today and tremendous untapped potential to bring it together. The sharing of information requires standardization – international standards. While there has been some progress in the development of standards, I urge people who are in charge to take an active role in embracing these requirements. This is where the internet can play an important role.

Finally, in order to make the data and knowledge sub-system more effective, we need to develop efficient text and biometric data mining engines. We need to develop engines – specifcially biometric API objects – that can sift through information more skillfully. I do not advocate the development of a single, centralized database and importing all of the available information from around the world. That is not the way our security framework is going to evolve, just like the world wide web does not operate through one main server. Instead, we see the evolution of web-like databases throughout the world with clearly defined information-sharing privileges; with the content owned and maintained by

the posting agencies. For the active government members of the Consortium, we need to work from a political point of view to bring this about. And as these modes are developing, , the power of this framework will multiply very rapidly.

Background Checks

Let us turn our attention to the second sub-system, which is called background checking. What we need throughout the security framework is a requirement for designating a "trusted identity". The "trusted identity" in my view is not a class distinction. It is not used to discern people into different classes. The "trusted identity" is a matter of national security. It is a matter of national security in the sense that it should be a mandated designation if your job is within the critical infrastructure of the nation. If your job involves airline crew, or airport personnel, you should be a trusted individual. Similarly, if you work in an energy facility such as a nuclear plant, you should be a trusted individual. We need a clear understanding of what the requirement for the "trusted identity" is, how should be mandated and to what it applies. For example, we should make available the notion of "trusted identity" to other programs, such as airline check-in or boarding. I should be able to go to an airline and ask to be qualified as a trusted traveler, and in that case the airline as standard procedure should do a background check that yields my classification as a trusted individual.

Some may argue that background-checking systems are already in place. I agree, albeit on a much smaller scale. Many of you may be familiar with the FBI's IAFIS – Integrated Automated Fingerprint Identification System. A large number of agencies use live scan fingerprint scanners to electronically transmit fingerprint data through channeling agencies for FBI background checks. Some of these channeling agencies include the Office of Personnel Management, for example, as well as commercial entities such as the American Banking Association.

Background checks have taken a much more visible role at least in the media and with the public. The FAA has created a more stringent mandate for background checks of airline crews and personnel. Some of you may remember back in November 2000 when the FAA mandated background checks on airport employees and personnel. However, this requirement applied only to new employees, and required that only the nation's top 20 airports comply within the year. It gave the rest – 400+ others – three years to comply.

After September 11, this changed. All employees, old and new, had to go through the background checking process. The new Transportation and Aviation Security Act of 2001 requires all airports to comply by November 2002. This means the creation of NIST records for 750,000 airport employees and crew personnel by November 2002, and, as a result of the high turnover in this industry, the creation of 250,000 new NIST records per year, thereafter. This new law has in itself major implications for the adoption of biometrics in airports and airlines.

To give you a sense of the opportunity, the yellow dots on the slide represent the fifteen or so airports that had adopted biometrics systems prior to September 11. Since then, there have been an additional 70-80 airports that have adopted live scan systems. The rate of adoption of live-scan systems among the various competitors is about ten a week.

This very fast adoption rate can be directly attributed to the FAA's updated background-check requirements.

So, what are the issues associated with this sub-system. As this is a common component and a very important element of the overall security framework, we need to broaden this requirement. Performing background checks on just airline crew and personnel may not be sufficient. We need to understand who are other individuals with critical jobs that impact our nation's security.

And as our background check requirements expand, we must ask ourselves, can the system as it exists, handle the required throughput? From a historical perspective, when these checks were done manually, nuclear power plants, for example, that used to hire several hundred people to clean up, were required to do background checks. But by the time they got the response back from the FBI, their job was already finished.

Another key performance factor is communication mechanisms. We have to understand that these background checking systems were developed at a time when mechanisms for communication such as web based XML, did not exist. Rather, existing mechanisms tend to rely on FTP, which is now considered out of date.

Finally, we need to pull together the broad range of information that we have. Today, background checks are conducted primarily using fingerprints. After September 11, the FBI started accepting mug shots. So as more and more records have both facial and finger data, we should be able to use the combined information in a more cohesive manner. A final question for consideration in this area, and one that I don't have an answer to, is how often do we conduct a background check on an individual. These issues are all critical if we are to use background checks as an integral component in the overall framework for homeland security.

"Trusted Identity" and Privileged Access

We talked about data and knowledge systems, the foundation for the security framework. We talked about the process and requirements for background checks. We now need to turn our attention to the notion of the "trusted identity" and establish who is entrusted and who is not. We need to look at with can be done with that designation. The "trusted identity" can be granted a set of privileges, such as expedited border clearance and automated access to certain facilities.

However, before we get too far, I want to emphasize that the "trusted identity" data need not reside in national database. When airport crew and personnel submit their records for background checks, for example, the information is not archived. As long as all eligible individuals are subject to uniform "trusted identity" standards, the entity administering the privilege, whether commercial or government, can maintain a separate archive. This may also be necessary because of privacy issues, however, the hope is that we will end up with a multi-purpose "trusted identity" designation.

How does this sub-system work? How does the "trusted identity" provide privileged access? The way we envision it, this is nothing more complicated than transaction

engines with biometric point-of-action sensors. This is a sub-system that checks identity, verifies authorization level, and most importantly, creates audit trails. This is no more complicated than commercial point-of-sale systems. If you look at VISA, for example, VISA has been building an engine capable of handling 100 billion complex transactions a year. Compare that to the 530 million biometric entries in the U.S., we are not looking at a huge amount.

Despite the example I just gave, I do not think the adoption of biometrics is going to evolve with transactions initially. The first adoption cycle will be in physical access, with particular emphasis on the transportation sector. Let us take a close look at the airline industry. Once they are comfortable with using biometrics for employee access, why not provide access to their frequent flyers?

Criminal and terrorist detection – "watch lists"

We all agree that with high probability we will still be left with a large fraction of the traveling population of those traveling from abroad who do not have any privileges or "trusted" identity designation. How do you maintain a level of security and continue to screen against criminals? The fact is, improved intelligence has been yielding terrorists' identities, that of facial images of course – of terrorists and criminals.

In a few slides, I will provide a a fraction of the information that is available to us. These images come from what is known as the FBI's Most Wanted. Some are terrorists, fugitives and criminals, but this list doesn't include international fugitives.

This list is dynamic. Most recently, the FBI put out a new list of 20 more people that they would like us to keep an eye out for. So as you can see, terror is not faceless. These images contain identity information and face-prints that can be used to screen against these individuals. In controlled areas, for example, where people have to go to a metal detector to board a plane, we can build mechanisms that ensure that people need to have their face captured as they walk through. This does not guarantee you, just like metal detectors and luggage scanners do not provide a guarantee that we are going to capture every terrorist in the system. At even a 50 to 60 percent effective rate – meaning interception rate – this is a mechanism can help deter crime and terror.

The watch list can also be used to examine ID documents. Full-page ID document scanners such as the ones shown in this slide, can scan the full page of the ID document and extract the facial image to match against a watchlist database. These document scanners can also be used to create a manifest that can be verified automatically. Putting one of these devices at each airline check-in counter will allow them to keep track of, and filter out, potential terrorists from boarding planes in the first place.

A comparable system of this kind developed after September 11 was adopted by the Dominican Republic for operation in 120 points of entry. Every person that goes into the country gets his/her ID document scanned against a national watch list database.

Beyond checkpoint and document surveillance, these watch lists can also be used for on-demand identification. If there is reason to suspect that an individual is a terrorist or a criminal, you can submit the individual's fingerprint and photo for search against the watch list database and bring the information back in real time. This is not a far-reaching concept. In California, during the first two months of operation, a system of this type yielded more then 100 positive identifications of criminals, 15 with outstanding warrants.

This area of watch list surveillance is a new branch of the biometrics applications domain. We have little industry experience. We need a national effort that can help us establish principles of operation, performance expectations and certification standards. Funding for ongoing development is necessary. This is a national priority and should not be thought of any differently than the kind of effort that went into developing luggage scanners and metal detectors. The only difference we face today is urgency. We are here today, as an industry, as a nation, faced with a challenge, a focused threat and we need to respond.

Challenges

Speaking of challenges, to this point, I have spoken mostly about the opportunity for the biometric industry to play a pivotal role in enhancing homeland security. However, I do not want to leave you with the impression that this opportunity is without difficulties. We have some serious challenges, not the least of which is the development of a system architecture. But I will leave that for another day. Today, I will focus on several key issues that government agencies have already brought to my attention – performance, expectations and privacy.

In the area of performance, we should be honest with ourselves. The accuracy of biometrics is less than desired. That is a fact. We have to less than ideal false acceptance, false rejection and failure to acquire rates. What compounds the problem is, we can not predict when these failures are going to happen. You, as an agency and as an end user, recognize that false accept, false reject and failure to acquire rates as a liability and we, as an industry have to transfer that liability into well-defined usage parameters. What can we do?

By combining biometrics, we can address performance issues in a way that meets realistic expectations. For example, some in the industry are considering what is called multibiometrics. Whenever this term is used, the implication is the use of layered biometrics, however, this is not what I am talking about. Layered biometrics will not necessarily improve performance. Let me explain why.

Layered biometrics means using two independent systems – both giving decisions – that are combined to yield a final result. Using face and finger as an example, a facial match comes up as a "yes" response, a finger match comes up as a "no" response, the end result is "no". The decision making process can only be determined by "and" and "or" functionalities, and can only yield a "yes" or "no" response, with no degree of certainty.

However, rather than taking only "yes" and "no" decisions, and instead, taking advantage of scoring mechanisms, one can determine the "degree" or "probability" of a match. By using critical properties in multiple biometrics, scores from two biometrics can be taken and combined to produce a decision that is much more improved and dynamic than either a single biometric or layered approach will yield.

This is called fusion. By fusing biometrics together, performance rates are dramatically improved, one can redundant layering and create "spoofing" countermeasures more effectively. It becomes harder for someone to manipulate the system. This slide shows the result of a real-world testing environment where the scores of two biometrics were fused to produce enhanced accuracy. Note the difference between the fused scores as opposed to the layered results.

Expectations. I have been at many meetings where people are seeking false reject rates at zero, false accept rates at zero, failure to acquire rates at zero and all at a cost of zero. That is the one that hurts me the most. The cost as equal to zero. This is not going to happen. We are not going to be able, as an industry, regardless of how much progress we make, regardless of the investment we make, to meet these expectations. We have to accept that technology has limitations and we must build systems that take these limitations into account.

For example, we need to invest in exception handling mechanisms. What happens when a biometric system fails? There needs to be a human backup mechanism in place. In the commercial arena, companies have customer call centers to provide assistance with their products. We also need to have customer satisfaction. We need to make intelligent decisions and focus our attention on only specific subjects. We do not want to needlessly harass anyone. So we need to be focusing on what triggers the backup mechanism.

.

All this being said, the final and biggest challenge in my opinion is privacy. With time and distance from September 11, I believe claims of "Big Brother" will resurface. There will be organizations that will be opposed to biometric systems despite the fact that they provide an added measure of security. The next few months and years will bring continued dialogue on the issue of national IDs. Will we move one way or another? The development of national standards for identity, is an element that will affect the development of our homeland security framework. We can deliver improved security without a national ID, but not without national standards for identity. We may be better off with a National ID. But that is not the requirement.

Oversight mechanisms. Will there be agencies who are tasked with overseeing the implementation of biometrics by other agencies? Do we need a privacy ombudsman? What happens if the system is misused? What is the recourse? What are the rights that the public has?

Privacy is an issue that we must address collectively as an industry, as end users and as a community. I have avoided throwing pitches during the course of this talk, but I believe I ought to give this one plug now to the IBIA. The International Biometric Industry Association has been playing a critical role on behalf of the industry in the area of

privacy, and they will continue to be an important advocate in the public policy arena. So please join them today.

Conclusion

In conclusion, I believe the association of identity with actions and credentials should be the framework of our homeland security strategy. I believe biometric technologies are central to that strategy. I also believe the technology is ready to meet realistic performance expectations.

Again, I plead with those agencies and entities that are in charge of developing this framework to focus on developing the platforms and standards before the individual operating sub-systems. My concern is that by focusing initially on the latter, we will end up developing stand-alone vertical systems that do not integrate. If we start by working on the platform, we will have be better able to create a scalable, complex security system down the line. I also believe the model architecture I have outlined before can evolve from existing systems.

Finally, I will leave you with this one point to consider. Over the last five months, we have seen a lot of action, however, this should not be confused with progress. Action does not mean progress. To make progress, we need to coordinate our specific actions with overall national priorities and objectives. A lot needs to get done. The industry is ready to step up to the challenge. Let us get to it.

Thank you for your attention.